Job Aid

Pre-Installation Network Planning Forms--S8700 Media Server

S8700 Media Server with an Avaya™ G600 Media Gateways
S8700 Media Server with Avaya™ MCC1/SCC1 Gateways

Before you install and configure an Avaya media server, complete the pre-installation planning forms.

Allow up to 4 hours to complete the forms. If you do not have this information complete, DO NOT BEGIN THE SERVER CONFIGURATION. DO NOT GUESS AT THESE NUMBERS. To do so could corrupt the customers network.

Review these planning forms with and get the data to fill it out from the customer corporate **LAN administrator**.

Some items in the planning forms are preceded by an alphanumeric reference marker. These reference markers, for many items, are included on Figure 1 and 2. The reference markers in the figures will help users to understand where items are configured. In addition, the reference markers are listed in Appendix A along with additional information about particular items.

Default values provided in the planning forms:

For Multi-Connect configurations many entries have default values because the control network is dedicated and provided by Avaya. It is strongly recommended that you use these defaults for the Multi-Connect configurations.

- The customer corporate LAN administrator may require you to change IP addresses to prevent conflicts with existing endpoints on the corporate LAN. Make precise notes of any changes and follow instructions exactly.

For IP Connect configurations very few entries can use default values. Because the IP Connect configuration uses the customer's non-dedicated network for both control and voice bearer, unique entries must be obtained from the customer corporate LAN administrator.

- Entries that can use default values for IP connect configurations will be specifically noted in the planning forms.

CAUTION:

It is crucial to coordinate the IP addresses that will be used with your Avaya media server with those on the enterprise LAN. If you specify an Ethernet address for the Avaya server component that conflicts with another Ethernet endpoint, the resulting problems with traffic on the local area network may be extremely difficult to diagnose and resolve.

These planning forms consist of the following sections:

- QoS Policy
- Logins required for installation
- Customer LAN Connectivity Test Information
- S8700 Configuration to be installed
- License and Registration Data
- Avaya S8700 Media Server configuration
- Other Media Server complex components
- IPSI IP Addresses
- Other Interfaces
- Appendix A Additional Information

QoS Policy

The network administrator must define the quality policy for telephony applications on the corporate enterprise network.

QoS Design Background

At layer 2 (802.1p/Q)

1a Will VLANs and Priority be used? (Y/N)_____

If Yes:

- **1b** What priority (6 recommended)_____
- **1c** What VLAN(s)_____
  (Show VLAN assignment by Subnet if not consistent across the Corporate Enterprise LAN)
- **1d** Will VLAN IDs for the server be tagged in the telephony product (e.g. S8700, S8300, G600, G700) or by the Ethernet switch?_____
- **1e** Will priority be tagged in the telephony product or by the Ethernet switch?_____
- **1f** Will VLAN IDs for the IP telephones be tagged by the telephones or by the Ethernet Switch?_____
  _____
  (If by Ethernet switch, configure VLAN IDs in the DHCP server)

1g Will Diffserve be used on IP connections? (Y/N)_____
If Yes:

- **1h** What Diffserve Value for Telephony will be used?_____
  (Recommend 46)

1i Will RSVP be used? (Y/N)_____
If Yes:

- **1j** What Refresh time?_____
- **1k** What Retry?_____
- **1l** What Profile?_____

Logins required for installation

S8700 Media Server and/or S8300 configured as LSP

Avaya Installation Personnel

- **craft** - Used for configuring and administering the S8700 server and access to Avaya MultiVantage software. For initial installation appropriate default passwords should be obtained through training. NOTE: After the authentication file is loaded on the S8700 server this login will be Access Security Gateway (ASG) protected, i.e. challenge and response.

Business Partner Personnel

- **dadmin** - Used for configuring and administering the S8700 server and access to Avaya MultiVantage software. For initial installation appropriate default passwords should be obtained during training.

G700 Media Gateway

Layer 2 switching processor

All personnel use:

- **root** - Used to configure the layer 2 switching processor and add additional users. The default password will be obtained during training

Media Gateway Processor (MGP)

All personnel use:

- **Session command** - Access to the MGP will generally be via the ‘session’ command after login to the Layer 2 switching processor is completed. Telnet sessions to the MGP can be established after addresses are configured. User authentication for these telnet sessions will be done by the Layer 2 switching processor. Any valid login (root or logins created by root) can be used to login to the MGP directly.

IP Server Interface Circuit Pack

All personnel use:

- **craft** - Used to set the IP address, subnet mask, a gateway on the IPSI circuit pack. The default password will be obtained during training.

Avaya Ethernet switches (if equipped)

All personnel use:

- root - Used for configuring the P333/334 switches supplied as control network switches. At initial installation the password for these devices is available in the user guide supplied with the switch.

Powerware 9125 UPS

All personnel use:

- When directly connected to the serial port on the ConnectUPS™ SNMP Module a login and password are not required. However, if the ConnectUPS™ SNMP Module has been previously configured to communicate with a modem a password is required to reconfigure it. The default password is available in the user guide supplied with the device.

Customer LAN Connectivity Test Information

For media servers that will be connected to a customer's corporate LAN testing will be required to verify connectivity. Obtain, from a customer representative, an IP address for a host on the customer's network. If Domain Name Service (DNS) is operational on the customer's network also obtain a DNS name for the host. NOTE: The DNS name and address will only be used as a target for a 'ping' operation. Login and password information for the host machine will **NOT** be required.

Customer host machine IP address_____

Customer host machine DNS name_____

S8700 Configuration to be installed

S8700 Media Servers can be installed in an IP Connect configuration or Multi-Connect configuration.

The IP connect configuration uses the corporate (customer) enterprise LAN to transport both control and voice bearer messages to and between Port Networks (PN). IP connect is available in the Duplex reliability configuration, i.e. duplicated media servers with a simplex non-dedicated (customer) network.

The multi-connect configuration uses a dedicated IP network to transport control messages to the PNs. A traditional Center Stage Switch (CSS) or Asynchronous Transfer Mode (ATM) switch is used to transport voice bearer traffic between PNs. Multi-Connect is available in three different reliability configurations.

- Duplex: Duplicated media servers; simplex (control network A) dedicated control network and simplex voice bearer network (CSS or ATM).
- High: Duplicated media servers; duplicated (control network A and B) dedicated control network; simplex voice bearer (CSS or ATM).
- Critical: Duplicated media servers; duplicated (control network A and B) dedicated control network; duplicated voice bearer network (CSS or ATM).

2a Enter the server configuration (IP-Connect or Multi-Connect) that will be installed {}:_____

S8700 Media Server placement

Servers may either be co-located (100 meters or less apart) or separated (greater than 100 meters but less than 10 kilometers) for disaster recovery purposes. This is important in that some entries in the configure server screens may be different depending on whether the servers are co-located and on the same subnet or separated and on different subnets. See item **2i**.

When servers are separated by more than 100 meters media converters will be required to extend Ethernet connections between servers. Other hardware may be required depending on the reliability configuration installed and the placement of control network switches (Multi-Connect configurations).

2b Enter whether the servers are co-located or separated {co-located}: _____

Software Release - Field Updates - Firmware Versions

2c Enter the software release that should be installed on the S8700 Media Servers{}:_____

2d Enter any field update numbers that should be installed on the S8700 Media Servers{}:_____

2e Enter the firmware version that should be installed on the TN2312 IPSI boards{}:_____

2f Enter the firmware version that should be installed on the TN799DP CLAN boards{}:_____

2g Enter the firmware version that should be installed on the TN2302AP Media Processor boards{}:_____

2h Enter the firmware version that should be installed on the TN2501AP Voice over LAN boards{}:_____

License and Registration Data

The following information will be required when using the either the Remote Feature Activation (RFA) web site or the Automatic Registration Tool (ART) web site.

RFA Data

3a Avaya SAP Order number{}: _____

3b Serial Number of 'Reference' TN2312 IP Server Interface (IPSI) circuit pack{}: _____
This serial number may not be available until delivery of equipment. This serial number is used in the creation of the license file that will be used on the S8700 Media Server. The IPSI circuit pack that will be closest, from a logical data point of view, to the media servers should be selected. This will decrease the amount of intervening equipment that could cause a lapse in communication with the reference IPSI.

NOTE:
ASG Product ID (PID) numbers will be obtained by RFA and incorporated into the S8700 servers via the license file. Alarm Product ID numbers will be provided, via the 'install script', by the Automatic Registration Tool. The Alarm PID will be entered during installation via a bash command (productid).

Automatic Registration Tool (ART) Data

ART requires this information to generate a skeleton MAESTRO record for the S8700 Media Server installation. ART will provide the following information to the user:

- Two Avaya IP addresses to configure into the servers. See item(s) **11a, 11b** under the ''For the Set Modem Interface screen'' on page 18

Co-located Servers
3c Full telephone number for the line used to access the Media Servers modem{}:_____

Separated Servers
3d Full telephone number for the line used to access Media Server 1 modem{}: _____

3e Full telephone number for the line used to access Media Server 2 modem{}: _____

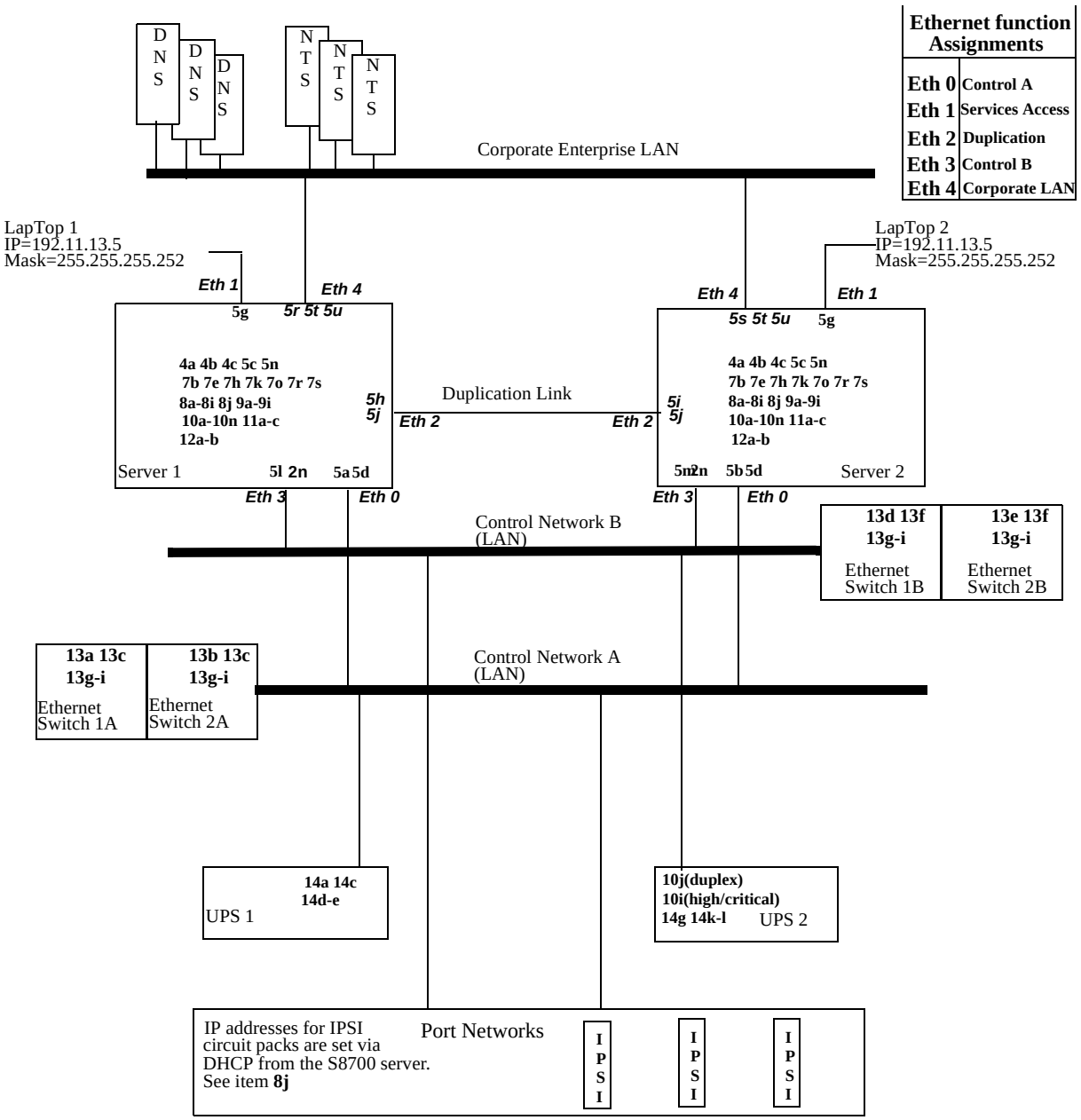

Figure 1. Multi-Connect Component Connectivity - High/critical reliability, dedicated control network

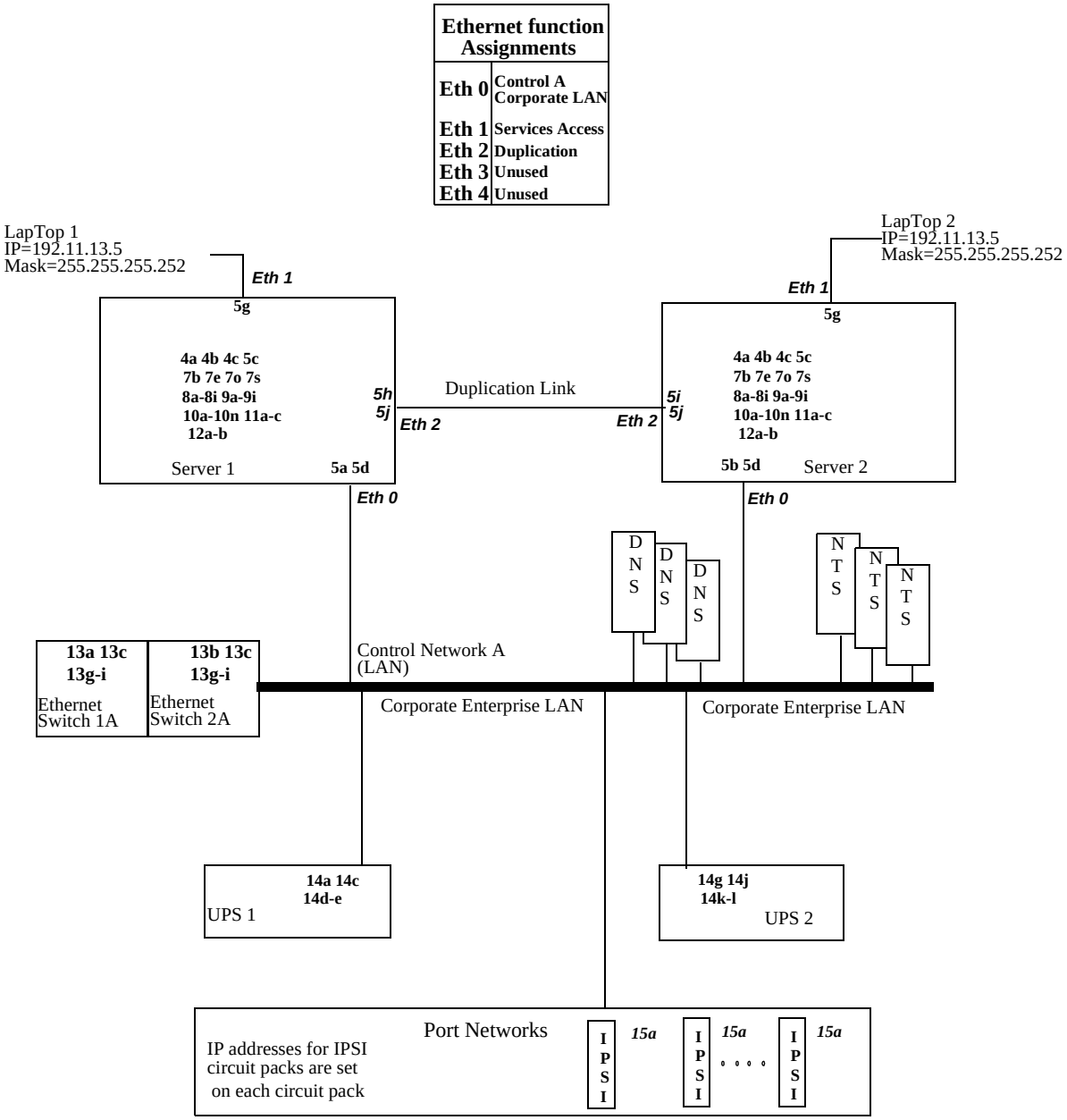

Figure 2. IP Connect Component Connectivity - Duplex, non-dedicated control network

Avaya S8700 Media Server configuration

The following planning form items are arranged in the order in which they are needed during server configuration. For an illustration of these items, see Figure 1 on page 7 for Multi-Connect or Figure 2 on page 8 for IP Connect. Each entry is identified with an alphanumeric reference.

For the Copy Settings screen

Screen 1 Select Configuration Method

Use this screen to select the method for configuring the server.

There are three options for configuring a server. During the configuration one of the three will be selected. A brief description of each of the options is included here for clarity.

- Configure all services using the wizard. This option will continue with the Set Identities screen and step through each subsequent screen in order. This option should always be used for the first server installation. NOTE: This is **not** the Avaya Installation Wizard. This **is** the traditional, step by step, configure server process.
- *Configure individual Services.* This option opens a screen that allows the user to individually select any one of the subsequent configure screens and go directly to it. This option will generally be used after software upgrades to populate added fields/screens. This option can also be used, after initial configuration, to go directly to a screen and change data.
- *Copy configuration information from the duplicated server.* This option opens a second screen to enter data for the duplication link. See items **5h-j** below. This option allows the user to copy information from an already configured server. This option will only be used to configure the second server of an installation. NOTE: This option requires that both servers have the same issue of software, the duplication cable between servers connected, and the duplication interface up on the server being copied from.

2i Server Separation (See item **2b**)

The corporate LAN interface of both servers is on the same subnet?{}____
NOTE: When the servers are on different subnets the ‘Active Server’ IP address will **not** be configured in subsequent screens.

For the Set Server Identities screen

NOTE:
When the servers are co-located they must be on the same subnet. When the servers are separated they may be on different subnets.

Server names

DEFAULTS
There are no defaults for these items. These items should be completed for both server configuration types (Multi-Connect and IP Connect)

These names should also be administered on any relevant corporate DNS servers. This information **must** be supplied by the corporate LAN administrator. Do not guess at a name, it could conflict with an existing name. Spaces are not allowed.

4a Name of server 1{}: _____

4b Name of server 2{}: _____

4c Active server name{}: _____
Not applicable if server separation is implemented and the servers are on different subnets.

Ethernet interface functions

The Ethernet function assigned to a physical interface jack are flexible. There are five physical interface jacks (Ethernet 0 through Ethernet 4) that can be assigned on the S8700 Media Server. There are up to five different functions that need to be assigned to a physical jack. They are:

- Control Network A (CNA), provides network for transmission of control messages between servers and port networks.
- Control Network B (CNB), provides duplicated (high/critical reliability only) network for transmission of control messages between servers and port networks.
- Duplication link, provides Ethernet duplication link between servers.
- Service port, provides direct Ethernet connection for service.
- Customer corporate LAN, provides access to servers from the corporate LAN.

Depending on which configuration and which reliability option is installed the Ethernet function assignment will vary.
Multi-Connect
With the Multi-Connect configuration, CNB is only provided for high and critical reliability configurations; the others are always present.
IP Connect
With IP Connect configurations the CNA and Corporate LAN functions are provided via the customers LAN. Consequently, both of these functions are assigned to one Ethernet Interface. Also, IP Connect is only available in a Duplex configuration which doesn't use CNB.

NOTE:
For Ethernet interface functions, always use the defaults unless specifically instructed to do otherwise. Physical cabling will have to match what is entered here.

4d Control Network A {Ethernet 0}:_____
Use the default for all configurations.

4e Services Port {Ethernet 1}:_____
Use the default for all configurations.

4f Server Duplication Link {Ethernet 2}:_____
Use the default for all configurations.

4g Control Network B {Ethernet 3}:_____
Multi-Connect; Duplex configuration: set this entry to Unused.
Multi-Connect; High and critical configurations: use the default

IP Connect: Duplex configuration: set this item to Unused.

4h Corporate LAN: {Ethernet 4}:_____
Multi-Connect; All configurations: use the default
IP Connect; Set this entry to Ethernet 0

For the Configure Ethernet Interfaces screen

Ethernet 0:

DEFAULTS
Multi-Connect; Duplex/High/Critical: Control Network A. Use the defaults.

IP-Connect; Duplex non-dedicated control network: Control Network A **and** Corporate LAN. Do not use the defaults,
Obtain addresses from the corporate LAN administrator.

5a Server 1 IP address on control network A: {198.152.254.201} _____
The same data will be entered at **14c, 14j(Duplex)**

5b Server 2 IP address on control network A: {198.152.254.202} _____

5c Active server IP address on control network A: {198.152.254.200} _____
The same data will be entered at **13c.** Not applicable if server separation is implemented

5d Subnet mask for control network A: {255.255.255.0} _____

5e Speed of link (10 or 100 megabit, full or half duplex): {autosense} _____
This entry must match the setting of the other end of the link. This is a critical item. If this entry is set to ‘autosense’ but the port at the other end is set to 100Mps/Full duplex it will result in a ‘duplex mismatch’ and cause error conditions and degradation of service. Generally all devices default to autosense (servers, Avaya data switches, IPSI circuit packs). For IP connect configurations careful coordination with the corporate LAN administrator will be required.

5f VLAN 802.1q priority tagging: {off} _____
Note: Tagging should be set the same on both control networks

Ethernet 1:

DEFAULTS
Service port
The address and subnet for this interface are fixed and not changeable.

5g Service IP address for every Avaya media server: 192.11.13.6

Subnet mask: 255.255.255.252

Ethernet 2:

DEFAULTS
Duplication link
All configurations should use the defaults.

5h Server 1 IP address on duplication link: {192.11.13.13} _____

5i Server 2 IP address on duplication link: {192.11.13.14} _____

5j Subnet mask for the duplication link: {255.255.255.252} _____

5k Speed of link (100 megabit, full duplex): {autosense} _____
This entry must match the setting of the other end of the link, i.e. the other server. This is a critical item. If this entry is set to 'autosense' but the port at the other end is set to 100Mps/Full duplex it will result in a 'duplex mismatch' and cause error conditions and degradation of service. Both servers default to autosense and should be left that way.

Ethernet 3:

DEFAULTS
Multi-Connect; Duplex configuration: Unused. Leave these entries blank.
Multi-Connect; High/Critical configuration: Control network B. Use the default entries.
IP Connect; Duplex configuration: Unused. Leave these entries blank

5l Server 1 IP address on control network B: {198.152.255.201} _____

5m Server 2 IP address on control network B: {198.152.255.202} _____
The same data will be entered at **14i (High/Critical)**

5n Active server IP address on control network B: {198.152.255.200} _____
The same data will be entered at **13f.** Not applicable if server separation is implemented.

5o Subnet mask for control network B: {255.255.255.0} _____

5p Speed of link (10 or 100 megabit, full or half duplex): {autosense} _____
This entry must match the setting of the other end of the link. This is a critical item. If this entry is set to ‘autosense’ but the port at the other end is set to 100Mps/Full duplex it will result in a ‘duplex mismatch’ and cause error conditions and degradation of service. Generally all devices default to autosense (servers, Avaya data switches, IPSI circuit packs).

5q VLAN 802.1q priority tagging: {off} _____
Note: Tagging should be set the same on both control networks

Ethernet 4:

DEFAULTS
Multi-Connect; All configurations, dedicated control network: Corporate LAN. Obtain addresses from the customer corporate LAN administrator.
IP Connect; Duplex configuration, non-dedicated control network: Unused. Leave these entries blank.

5r Server 1 IP address on the corporate LAN: _____

5s Server 2 IP address on the corporate LAN: _____

5t Active server IP address on the corporate LAN: _____
Not applicable if server separation is implemented.

5u Gateway IP address for the corporate LAN: _____

5v Subnet mask for the corporate LAN: _____

5w Speed of link (10 or 100 megabit, full or half duplex): {autosense} _____
This entry must match the setting of the other end of the link. This is a critical item. If this entry is set to ‘autosense’ but the port at the other end is set to 100Mps/Full duplex it will result in a ‘duplex mismatch’ and cause error conditions and degradation of service. Careful coordination with the corporate LAN administrator will be required.

5x VLAN 802.1q priority tagging: {off} _____

For the Control Switches and UPS screen

Configure Local Survivable Processor

Select one of the following (**6a, 6b, 6f**):

6a This is NOT a local survivable processor:___

6bThis is a local survivable processor with a S8700 media server as the primary controller:___

6c CLAN IP address of the primary controller (required):_____

6d IP Address of server 1(required):_____

6e IP Address of server 2 (required):_____

6f This is a local survivable processor with a S8300 media server as the primary controller___

6g IP address of the primary controller (required)_____

Specify the Ethernet switches for each control network

DEFAULTS
Multi-Connect; Duplex configuration: Use the defaults for items **7a -7g**.
Multi-Connect; High/critical configurations: Use the defaults for items **7a - 7m**.

IP Connect; Duplex configurations: Does not apply. Leave these entries (**7a - 7m**) blank.

7a Number of Ethernet switches per control network: {1} _____
Note: Doesn't apply to non-dedicated control networks

7b Ethernet switch 1 IP address on control network A: {198.152.254.240} _____
The same data will be entered at **13a**

7c SNMP GET (read) community string: {public} _____

7d SNMP SET (write) community string: _____

7e Ethernet switch 2 IP address on control network A: {198.152.254.241} _____
The same data will be entered at **13b**

7f SNMP GET (read) community string: {public} _____

7g SNMP SET (write) community string: _____

7h Ethernet switch 1 IP address on control network B: {198.152.255.240} _____
The same data will be entered at **13d**

7i SNMP GET (read) community string: {public} _____

7j SNMP SET (write) community string: _____

7k Ethernet switch 2 IP address on control network B: {198.152.255.241} _____
The same data will be entered at **13e**

7l SNMP GET (read) community string: {public} _____

7m SNMP SET (write) community string: _____

Specify the UPS units for each control network

Note: There are always 2 UPS units. For a Duplex reliability configuration they both have addresses on Control Network A. For the High/Critical reliability configuration UPS 1 will have an address on control network A and UPS 2 will have an address on control network B. **UPS 1 MUST** supply power for media server 1 and **UPS 2 MUST** supply power for media server 2. If this is reversed a problem (low battery) with the UPS supplying power to the standby server will cause the active server to be shutdown.

DEFAULTS
Multi-Connect; all configurations: use the defaults
IP Connect; Duplex configuration: use corporate LAN administrator provided addresses

7n Number of UPS units for the control network: {2} _____

7o UPS 1 IP address on control network A: {198.152.254.239} _____
The same data will be entered at **14a**

7p SNMP GET (read) community string: {public} _____

7q SNMP SET (write) community string: _____

High/Critical
7r UPS 2 IP address on control network B: {198.152.255.239} _____
The same data will be entered at **14f**

Duplex
7s UPS 2 IP address on control network A: {198.152.254.238} _____
The same data will be entered at ***14g***

7t SNMP GET (read) community string: {public} _____

7u SNMP SET (write) community string: _____

For the DNS and DHCP Server Configuration screen

DEFAULTS
Multi-Connect and IP Connect: Optional for all configurations.

If domain name service (DNS) servers are to be used, complete as many of the following fields as needed to set up DNS service and limit unresolved name searching. Fill out only as many server and search domain fields as are needed. These DNS servers are always on the customers corporate LAN. The S8700 servers do not provide domain name service:

8a DNS server 1 IP address: _____

8b DNS server 2 IP address: _____

8c DNS server 3 IP address: _____

8d DNS domain name: _____

8e Search domain name 1: _____

8f Search domain name 2: _____

8g Search domain name 3: _____

8h Search domain name 4: _____

8i Search domain name 5: _____

Specify whether the Avaya media server will provide DHCP service, for IPSIs, or whether IPSI IP addresses will be manually assigned:

NOTE:
For IP Connect configurations IPSI DHCP service **cannot** be activated, IPSI addresses must be manually (static) assigned. For Multi-Connect configurations it is highly recommended that IPSI DHCP service be activated.

8j Enable DHCP service on media servers: {yes} _____

For the Set Static Network Routes screen

Optional: Enter any static IP addresses specified by the customer's LAN administrator.

	IP address of endpoint server is trying to reach	Subnet mask used by all endpoints	Gateway IP address (optional)	Ethernet interface (optional)
9a				
9b				
9c				
9d				
9e				
9f				
9g				
9h				
9i				

For the Network Time Server screen

DEFAULTS
Multi-Connect and IP Connect; All configurations: There are no defaults, all information must be provided by the corporate LAN administrator. For more information about these entries see Appendix A.

10a Is a Network Time Server (NTS) available to be used as the time source? (Y/N) _____
If an external NTS is available, both servers in the S8700 Media Server complex should be administered to synchronize with it. Select the second radio button on the screen (**10c)** and fill in the fields detailed below on both servers.

10b This computer synchronizes with the duplicated server.___
If an external NTS is not available both servers should have this option selected. In this case Server 1 will always act as a Network Time Server and server 2 will synchronize with it.

10c Use these Network Time Servers:___
If a NTS is available, both servers in the S8700 Media Server complex should be administered to synchronize with it.

If NTSs are available, enter their DNS names or IP addresses

10d Primary NTS name or IP address: _____
10e Trusted Key _____(Leave blank if not used)

10f Secondary NTS name or IP address: _____
10g Trusted Key _____(Leave blank if not used)

10h Tertiary NTS name or IP address: _____
10i Trusted Key _____(Leave blank if not used)

10j Multicast Client Support? (Y/N): _____

Additional Keys
(Leave blank if not used)

10k Trusted Key:_____

10l Requested Key:_____

10m Control Key:_____

10n Will a *Keys file* be used (Y/N): ____
Note: If Yes, it must be supplied during this configuration step and should reside in the ***/var/home/ftp*** directory.

For the Set Modem Interface screen

DEFAULTS
Multi-Connect and IP Connect; All configurations: There are no defaults, entries **11a** and **11b** will be unique for each installation. This data will be supplied by the Automatic Registration Tool (ART).

Specify the IP address for each server's modem (this information must be provided by Avaya Services if a maintenance contract is in force):

11a IP address of the PPP dial-up link for server 1: _____

11b IP address of the PPP dial-up link for server 2: _____

11c Set International Modem Setting:__ (Check box)

Return routes are no longer required for Avaya service. The default return routes can be left:

Information	IP address	Subnet mask
11d Default Return Route Codes	135.9.0.0 135.17.0.0 135.39.0.0 135.60.0.0 198.152.171.0 198.152.171.0	255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.255.0 255.255.255.0

For the Configure Trap Destinations screen

DEFAULTS
Multi-Connect and IP Connect; All configurations: There are no defaults.

NOTE:
This screen is separate from the previous Configure Server screens. Access this screen from the main web interface page under the SNMP heading.

Specify Simple Network Management Protocol (SNMP) data trap destination. This information will allow the active server to send SNMP trap information to a Network Management System, i.e. CajunView.

12a IP address of SNMP trap receiver: _____

12b SNMP protocol version (1, 2c or 3): _____

Required for version 1:

12c Community name: _____

Required for version 2c:

12d Notification type (trap/inform): _____

12e Community name: _____

Required for version 3:

12f Notification type (trap/inform): _____

12g User name: _____

12h Security model (none, authentication, or privacy): _____

12i Authentication password (required for authentication and privacy model): _____

12j Privacy password (required for privacy model): _____

Other Media Server complex components

Ethernet Switch(s)

DEFAULTS
Multi-Connect; all configurations: Use the defaults.
IP Connect; Duplex configuration: Not used, leave these entries blank. For non-dedicated control network configurations it is the LAN administrators responsibility to properly administer the Ethernet switches

The following information will be configured directly in the Ethernet switch(s) and will only be used in dedicated control network configurations.

IP Address on control network A

13a Ethernet switch 1 IP address on control network A: {198.152.254.240} _____
Use IP address from entry **7b**

13b Ethernet switch 2 IP address on control network A: {198.152.254.241} _____
Use IP address from entry **7e**

Trap receiver destination on control network A

13c Trap receiver destination for both Ethernet switches on control network A: {198.152.254.200}_____
Use IP address from entry **5c**

IP Address on control network B

13d Ethernet switch 1 IP address on control network B: {198.152.255.240} _____
Use IP address from entry **7h**

13e Ethernet switch 2 IP address on control network B: {198.152.255.241} _____
Use IP address from entry **7k**

Trap receiver destination on control network B

13f Trap receiver destination for both Ethernet switches on control network B: {198.152.255.200}_____
Use IP address from entry **5n**

Community Strings for all Ethernet Switches

Switch 1 CNA
13g Get (read-only) community string: {Public}_____
Use the community string entered at **7c**.

13h Set (read-write) community string: {Public}_____
Use the community string entered at **7d**.

Switch 2 CNA (if equipped)
13i Get (read-only) community string: {Public}_____
Use the community string entered at **7f**.

13j Set (read-write) community string: {Public}_____
Use the community string entered at **7g**.

Switch 1 CNB (if equipped)
13k Get (read-only) community string: {Public}_____
Use the community string entered at **7i**.

13l Set (read-write) community string: {Public}_____
Use the community string entered at **7j**.

Switch 2 CNB (if equipped)
13m Get (read-only) community string: {Public}_____
Use the community string entered at **7l**.

13n Set (read-write) community string: {Public}_____
Use the community string entered at **7m**.

Uninterruptible Power Supplies

These entries are always required and will always be administered directly in the UPS units. UPS 1 supplies power to media server 1 and reports to media server 1 and UPS 2 supplies power to media server 2 and reports to media server 2. This is very important because if it is reversed a problem with a UPS will cause the wrong server to be shutdown.

UPS 1

14a UPS 1 IP address on control network A: {198.152.254.239} _____
Use IP address from entry **7o**

14b Subnet Mask for UPS 1 on control network A:{255.255.255.0}_____

14c Default Gateway for UPS 1 on control network A:{198.152.254.201}_____
Use IP address from entry **5a**

14d SNMP GET (read-only) community string: {public} _____
Use the community string entered at **7p**.

14e SNMP SET (read-write) community string: _____
Use the community string entered at **7q**.

UPS 2

High/Critical
14f UPS 2 IP address on control network B: {198.152.255.239} _____
Use IP address from entry **7r**

Duplex
14g UPS 2 IP address on control network A: {198.152.254.238} _____
Use IP address from entry **7s**

14h Subnet Mask for UPS 2 on control network A:{255.255.255.0}_____

High/Critical
14i Default Gateway for UPS 2 on control network B:{198.152.255.202}_____
Use IP address from entry **5m**

Duplex
14j Default Gateway for UPS 2 on control network A:{198.152.254.201}_____
Use IP address from entry **5a**

14k SNMP GET (read-only) community string: {public} _____
Use the community string entered at **7t**.

14l SNMP SET (read-write) community string: _____
Use the community string entered at **7u**.

IPSI IP Addresses

DEFAULTS
Multi-Connect
With Multi-Connect configurations it is highly recommended that Dynamic Host Control Protocol (DHCP) be enabled on the S8700 Media Servers to assign IPSI addresses. See item **8j**.
IP Connect
With IP Connect configurations, IP Server Interface (IPSI) circuit packs need to be manually programmed. Each Port Network (PN), to maximum of 64, will be equipped with an IPSI circuit pack. The IP addresses programmed into the IPSI circuit packs will be on the customers corporate LAN. For the purposes of these planning forms, gather enough addresses to provide one address for each ISPI. Replicate this page if more space is needed.
Figure reference number: ***15a***.

Port Network (PN)	IP Address	Subnet Mask	Gateway	Speed/ Duplex	VLAN ID

Other Interfaces

Control Lan (C-LAN - TN799DP), IP Media Processor (MP - TN2302AP), and Voice Announcement over Lan (VAL - TN2501AP) resources in the media gateway port networks require network configuration. Use the following table to gather required information for these interfaces.

NOTE:
These resources are not shown in the component connectivity figures. They will be configured in the MultiVantage software application using Avaya Site Administration.

NOTE:
G700 Media Gateways will require configuration in the MultiVantage software application. Refer to *Installation and Upgrades for Avaya™ G700 Media Gateway controlled by an Avaya S8700 Media Server (*555-234-100)

Resource Type (CLAN, MP, VAL)	DNS/ MultiVantage Name	USE	Port Network Location	IP Address	Subnet Mask	Gateway	Speed/ Duplex	VLAN	Firmware Version

Appendix A Additional Information

S8700 Configuration to be installed

Enter whether this will be a Multi-Connect configuration or an IP Connect configuration. This information will only required when a server is first configured or when a server has been reset to defaults.

For the Set Server Identities Screen

Server names

4a Enter a name that uniquely identifies server 1. Do not guess at a name. Coordinate this entry with the corporate LAN administration for Domain Name Servers (DNS).

4b Enter a name that uniquely identifies server 2. Do not guess at a name. Coordinate this entry with the corporate LAN administration for Domain Name Servers (DNS).

4c Enter a unique name that will be used to connect to the active server. This name and it's associated IP address (items **5c, 5n**) will connect to whichever server is active. Do not guess at a name. Coordinate this entry with the corporate LAN administration for Domain Name Servers (DNS). Not applicable if server separation is implemented.

Ethernet interface functions

The following entries will determine the physical interface (RJ45 jack) that a particular function will use. Always use the defaults unless specifically instructed to do otherwise. Physical cabling will have to match the assignments made here.

4d Choose an Ethernet interface for Control Network A.
Use the default for all configurations.

4e Choose an Ethernet interface for the service port.
Use the default for all configurations.

4f Choose an Ethernet interface for the duplication link.
Use the default for all configurations.

4g Choose an Ethernet interface for Control Network B.
Multi-Connect; Duplex configuration: set this entry to Unused.
Multi-Connect; High/Critical configurations: use the defaults
IP Connect; Always set this item to Unused.

4h Choose an Ethernet interface for the Corporate LAN (customer LAN).
Multi-Connect; All configurations: use the default
IP Connect; Set this entry to Ethernet 0

Configure Ethernet Interfaces

Ethernet 0

DEFAULTS
Multi-Connect; Duplex/High/Critical: Control Network A
IP-Connect; Duplex non-dedicated control network: Control Network A **and** Corporate LAN

5a Enter the IP address for Server 1 on Control Network A.

5b Enter the IP address for Server 2 on Control Network A.

5c Enter the IP address for the active server on Control Network A.
Not applicable if server separation is implemented.

5d Enter the subnet mask for Control Network A.

5e Enter the speed of the Ethernet 0 link.
This entry must match the setting of the other end of the link. This is a critical item. If this entry is set to ‘autosense’ but the port at the other end is set to 100Mps/Full duplex it will result in a ‘duplex mismatch’ and cause error conditions and degradation of service. Generally all devices default to autosense (servers, Avaya data switches, IPSI circuit packs). For IP connect configurations careful coordination with the corporate LAN administrator will be required.

5f Choose whether or not VLAN 802.1q priority tagging should be on or off in the server.

Ethernet 1

DEFAULTS
All configurations: Service port

5g This IP address is fixed and not changeable. It will always be 192.11.13.6 with a subnet of 255.255.255.252

Ethernet 2

DEFAULTS
Multi-Connect: Duplication Link
IP Connect: Duplication Link

5h Enter the IP address for Server 1
Multi-Connect and IP Connect; All configurations: Always use the default, Avaya reserved, address 192.11.13.13

5i Enter the IP address for Server 2
Multi-Connect and IP Connect; All configurations: Always use the default, Avaya reserved, address 192.11.13.14

5j Enter Subnet mask for the duplication link.
Multi-Connect and IP Connect; All configurations: Always use 255.255.255.252

5k Enter the speed of the link.
This entry must match the setting of the other end of the link, i.e. the other server. This is a critical item. If this entry is set to 'autosense' but the port at the other end is set to 100Mps/Full duplex it will result in a 'duplex mismatch' and cause error conditions and degradation of service. Both servers default to autosense and should be left that way.

Ethernet 3

DEFAULTS
Multi-Connect; Duplex configuration: Unused. Leave these fields blank
Multi-Connect; High/Critical configuration: Control network B. Use the defaults.
IP Connect; Duplex configuration: Unused. Leave these fields blank.

5l Enter the IP address for Server 1 on Control Network B.

5m Enter the IP address for Server 2 on Control Network B.

5n Enter the IP address for the active server on Control Network B.
Not applicable if server separation is implemented.

5o Enter the subnet mask for Control Network B.

5p Enter the speed of the Ethernet 0 link.
This entry must match the setting of the other end of the link. This is a critical item. If this entry is set to 'autosense' but the port at the other end is set to 100Mps/Full duplex it will result in a 'duplex mismatch' and cause error conditions and degradation of service. Generally all devices default to autosense (servers, Avaya data switches, IPSI circuit packs).

5q Choose whether or not VLAN 802.1q priority tagging should be on or off for this interface.

Ethernet 4

DEFAULTS
Multi-Connect; All configurations, dedicated control network: Corporate LAN
IP Connect; Duplex configuration, non-dedicated control network: Unused

5r Enter the IP address for Server 1 on the corporate (customer) LAN

5s Enter the IP address for Server 2 on the corporate (customer) LAN

5t Enter the IP address for the active server on the corporate (customer) LAN
Not applicable if server separation is implemented.

5u Enter the IP address for the gateway on the corporate (customer) LAN

5v Enter the subnet mask for the corporate LAN

5w Enter the speed of the Ethernet 4 link.
This entry must match the setting of the other end of the link. This is a critical item. If this entry is set to 'autosense' but the port at the other end is set to 100Mps/Full duplex it will result in a 'duplex mismatch' and cause error conditions and degradation of service. Careful coordination with the corporate LAN administrator will be required.

5x Choose whether or not VLAN 802.1q priority tagging should be on or off for this interface.

Control Switches and UPS

Configure Local Survivable Processor

Typically these entries will only be completed (with the exception of **6a**) on a G700 media gateway equipped with a S8300 media server that is going to be used as a local spare processor. One entry **6a, or 6b, or 6f** must be selected for every server type. When either **6b** or **6f** are selected the associated entries are required.

6a Select this entry if this is **NOT** a local survivable processor
Select this entry for the primary controllers of Multi-Connect or IP Connect configurations.

6b Select this entry if this is a local survivable processor with a S8700 Media Server as the primary controller

6c Enter the CLAN IP address of the primary controller. This is the address that is, or will be, administered on the 'change node-names' administration screen.

6d Enter the IP address for server 1 **of the primary controller**. This is **NOT** the server 1 IP address for this controller. This is the IP address of the server 1 that **this** server will take over for in the case of a failure.

6e Enter the IP address for server 2 **of the primary controller**. This is **NOT** the server 2 IP address for this controller. This is the IP address of the server 2 that **this** server will take over for in the case of a failure.

6f Select this entry if this a local survivable processor with a S8300 media server as the primary controller

6g Enter the IP address of the primary controller. This is **NOT** the IP address of this controller. This is the IP address of the S8300 server that **this** server will take over for in the case of a failure.

Specify Ethernet Switches for each control network

SNMP community strings for Ethernet switches and UPS units.

All of the S8700 Media Server component parts ship with default community strings for the Get (read-only) and Set (read-write) SNMP operations. It is important, for security purposes, to change these values to something other than the defaults.
The community strings act like a password. When a Get or Set is issued to a particular entity on the network the community string is included to validate the sender to the receiver of the Get/Set. Changing the community strings will help protect S8700 Media Server components from intrusion attempts. This is especially important in the case of the Set command, which has the ability to perform configuration and control operations. An example of how a Set command could be used maliciously would be it's capability to shutdown the loads supplied by the UPS unit. Community strings should be unique strings of characters and numbers. The community strings DO NOT have to follow any preset format. The community strings DO have to match exactly in the media server and peripheral unit (data switch/UPS).
For Example, entry 7c is the community string for the SNMP Get associated with the first Ethernet switch on Control Network A (CNA). Whatever unique string is entered for item 7c should be entered as the SNMP Get community string when the Ethernet switch itself is configured. The same holds true for items 7d,f,g,i,j,l,m,p,q,t,u. Whatever is entered here in the server should be entered in the corresponding peripheral switch or UPS unit.

7a Enter the number of Ethernet switches, per control network that will be equipped.
This entry does not apply to non-dedicated control networks.

7b Enter the IP address on control network A for the first Ethernet switch. This is the IP address for this switch on control network A. You would use this address if you wanted to telnet to this switch to administer it.

7c Enter the SNMP GET (read) community string for this switch

7d Enter the SNMP SET (write) community string for this switch

7e Enter the IP address on control network A for the second (if equipped) Ethernet switch. This is the IP address for this switch on control network A. You would use this address if you wanted to telnet to this switch to administer it.

7f Enter the SNMP GET (read) community string for this switch

7g Enter the SNMP SET (write) community string for this switch

7h Enter the IP address on control network B for the first Ethernet switch. This is the IP address for this switch on control network B. You would use this address if you wanted to telnet to this switch to administer it.

7i Enter the SNMP GET (read) community string for this switch

7j Enter the SNMP SET (write) community string for this switch

7k Enter the IP address on control network B for the second (if equipped) Ethernet switch. This is the IP address for this switch on control network B. You would use this address if you wanted to telnet to this switch to administer it.

7l Enter the SNMP GET (read) community string for this switch

7m Enter the SNMP SET (write) community string for this switch

Specify the UPS units for each control network

7n Enter the number of UPS units equipped. Unless other arrangements are made for uninterruptible power this entry should always be 2.

7o Enter the IP address for UPS 1 on control network A. This is the IP address for the SNMP module or functionality equipped in UPS 1 on control network A. You would use this address if you wanted to telnet to this UPS to administer it.

7p Enter the SNMP GET (read) community string for UPS 1

7q Enter the SNMP SET (write) community string for UPS 1

7r High/Critical configurations enter the IP address for UPS 2 on control network **B**.

7s For duplex configurations enter the IP address for UPS 2 on control network **A**.

For either reliability configuration enter the SNMP community strings for UPS 2

7t Enter the SNMP GET (read) community string for UPS 2

7u Enter the SNMP SET (write) community string for UPS 2

DNS and DHCP Server Configuration

8a Enter the IP address for DNS server 1.

8b Enter the IP address for DNS server 2.

8c Enter the IP address for DNS server 3.

8d Enter the DNS domain name.

8e Enter search domain name 1.

8e Enter search domain name 2.

8e Enter search domain name 3.

8e Enter search domain name 4.

8e Enter search domain name 5.

8j Enter whether or not DHCP service for IP Server Interface (IPSI) circuit packs should be enabled.
For IP Connect configurations DHCP service **cannot** be activated, IPSI addresses must be manually assigned. For Multi-Connect configurations it is highly recommended that DHCP service be activated.

Set Static Network Routes

9a-9i Enter any static IP addresses routes. These will be specified by the corporate LAN administrator.

Network Time Server

10a Enter whether or not a Network Time Server (NTS) is available
If a NTS is **not** available check option **10b**.
If a NTS **is** available check item **10c**. Both servers in the S8700 Media Server complex should be administered to synchronize with it.

10b Check this option if a NTS is not available.
If an external NTS is not available both servers should have this option selected. In this case server 1 will always act as a Network Time Server and server 2 will synchronize with it. If this option is selected skip the remaining NTS entries.

10c Check this option if a NTS is available.
If a NTS is available, both servers in the S8700 Media Server complex should be administered to synchronize with it.

10d Enter the name or IP address for the primary NTS
10e Enter a Trusted Key for this NTS. (Leave blank if not used)

10f Enter the name or IP address for the secondary NTS
10g Enter a Trusted Key for this NTS. (Leave blank if not used)

10h Enter the name or IP address for the tertiary (third) NTS
10i Enter a Trusted Key for this NTS. (Leave blank if not used)

10j Enter whether or not the media server should support Multicast Client Support
Typically, multicast is not used when network time servers are specified.

- Select Yes if the NTS routinely broadcasts its timing messages to multiple clients
- Select No if the Avaya media server is to poll (directly request the time from) the specified Network Time Servers.

10k Enter the Trusted Key. (Leave blank if not used.)

- Trusted keys function like a checksum to make sure the time packets are valid. Trusted keys that are entered with the entries for NTS (**10e, 10g, 10i)** or as a Requested key (**10l**) or Control key (**10m**) are automatically added to the list of trusted keys in the Trusted Key field. Typically, the only time an additional entry is added occurs when the Trusted key list is used with multicast authentication. Such is the case because no explicit trusted key entry is associated with the multicast option.
  - Specify additional trusted keys that this media server can use to authenticate time messages, if required by any of the other servers.
  - Use a blank space as a delimiter if there is more than one key (for example, 2 3 6 to specify valid keys 2,3, and 6) These numbers are associated with encryption codes in a “keys” file. See item **10n**.

10l Enter the Requested Key. (Leave blank if not used.)
This key allows an administrator to send a remote query request. Only 1 key is allowed in this field. A key entry here will automatically be added to the Trusted Keys (item **10k)**.

10m Enter the Control Key. (Leave blank if not used.)
This key allows an administrator to query and request changes to an NTS. Only 1 key is allowed in this field. A key entry here will automatically be added to the Trusted Keys (item **10k)**.

10n Enter whether or not a Keys file will be used.
If you specify keys in items **10e, g, i, k, l** you **must** provide a file named keys.install to allow the media server to communicate with the NTS. The keys.install file should be obtained from the corporate LAN administrator before the server is configured. The keys.install file must reside in the ftp home directory (/var/home/ftp) **before** the configuration is submitted. The keys.install file can be uploaded to the ftp directory using the Upload Files to Server link under the Miscellaneous heading of the Web Interface.
If a keys file is not installed until later, the Configure Server process will have to be run again in order for the server to recognize the keys.install file.

Set Modem Interface

Items **11a** and **11b** are always provided. When server separation is greater than 100 meters two telephone lines are equipped, one for each modem. When server separation is less than 100 meters one telephone line is provided and wired to both modems.

11a Enter the IP address of the PPP dial-up link for server 1. The default entry for this item will always be changed. Values for this item will be provided by the Automatic Registration Tool (ART).

11b Enter the IP address of the PPP dial-up link for server 2. The default entry for this item will always be changed. Values for this item will be provided by the Automatic Registration Tool (ART).

11c Set International Modem Setting.

11d Return routes are no longer required for Avaya service.
If a service provider, other than Avaya, is used and they require return routes they will have to provide them.

Configure Trap Destinations screen

12a Enter the IP address of the SNMP trap receiver. This is the IP address of the corporate Network Management System, i.e. CajunView. Traps or Informs will be forwarded to this destination so that equipment may be monitored. This entry must be entered in dotted decimal notation (not DNS name).

12b Enter the SNMP protocol version (1, 2c or 3) that will be used with this destination (**12a**).
Depending on which protocol version is selected, fill out the appropriate entries **12c** or **12d,e** or **12f-j**.

Version 1

12c Enter the Community name
Enter a text string to provide security for SNMP messages. You can use any characters except: ‘\&,’ ” (single back-quote, backslash, ampersand, comma, single quote, double quote).

Version 2c

12d Enter the Notification Type (trap/inform)
Select either trap or inform.

- Trap - indicates an alarm or notable event condition. These include potentially service-disrupting activities, such as activation of UPS power, or events such as when anew device is added.
- Inform - An acknowledged trap. The receiver of the trap is expected to respond with an SNMP message acknowledging receipt of the trap.

12e Enter the Community Name
Enter a text string to provide security for SNMP messages. You can use any characters except: '\&,' " .

Version 3

12f Enter the Notification Type (trap/inform)
Select either trap or inform. See item **12d** for details.

12g Enter the User name
Enter a text string that indicates the user that is authorized to send traps or informs to the destination. The name can contain any characters except: '\&,' " (for example: Jane Doe).

12h Enter the security model (none, authentication, or privacy)
Select the level of security to use when sending v3 traps or informs.

- None: no additional information is needed. Traps or informs are sent in plain text without a digital signature.
- Authentication: an authentication password must be given. SNMP v3 uses this pass phrase to digitally "sign" v3 traps using MD5 protocol (associate them with the user).
- Privacy: both an authentication password and a privacy password must be given in order to provide user-specific authentication and encryption. Traps or informs are signed as above and also encrypted using Data Encryption Standard (DES) protocol.

12i Enter the Authentication password (required for the authentication and privacy models)
Enter a text string at least 8 characters long to provide user-specific authentication by means of a digital signature. The pass phrase can contain any characters except: '\&,' "

12j Enter the Privacy password (required for the privacy model)
Enter a text string at least 8 characters long to provide user-specific authentication and trap encryption. The pass phrase can contain any characters except: '\&,' "

Other Media Server complex components

Ethernet Switch(es)

IP Address on control network A

13a Enter the IP address for Ethernet switch 1 on control network A. This entry will be the same as **7b**.

13b Enter the IP address for Ethernet switch 2 on control network A. This entry will be the same as **7e**.

Trap receiver destination on control network A

13c Enter the IP address for the trap receiver for both switches on control network A. This entry will be the same as **5c**.

IP Address on control network B

13d Enter the IP address for Ethernet switch 1 on control network B. This entry will be the same as **7h**

13e Enter the P address for Ethernet switch 2 on control network B. This entry will be the same as **7k**

Trap receiver destination on control network B

13f Enter the IP address for the trap receiver for both switches on control network B. This entry will be the same as **5n**.

Community Strings for all Ethernet Switches

13g Enter the community SNMP strings for Read Only access for all Ethernet switches.

13h Enter the community SNMP strings for Read/Write access for all Ethernet switches.

13i Enter the community SNMP strings for Trap generation for all Ethernet switches.

Uninterruptible Power Supplies

UPS 1

14a Enter the IP address for UPS 1 on control network A. This entry will be the same as **7o**.

14b Enter the Subnet Mask for UPS 1 on control network A.

14c Enter the Default Gateway for UPS 1 on control network A. This entry will be the same as **5a**.

14d Enter the SNMP GET (read) community string.

14e Enter the SNMP SET (write) community string.

UPS 2

14f For High and Critical reliability configurations enter the IP address for UPS 2 on control network B.This entry will be the same as **7r**.

14g For Duplex reliability configurations enter the IP address for UPS 2 on control network A. There is no control network B in Duplex reliability systems so UPS 2 will require an address on control network A. This entry will be the same as **7s.**

14h Enter the Subnet Mask for UPS 2.

High/Critical
14i For high and critical reliability configurations enter the Default Gateway for UPS 2 on control network B. This entry will be the same as **5m**.

Duplex
14j For duplex reliability configurations enter the Default Gateway for UPS 2 on control network A. There is no control network B on duplex reliability configurations so a Default Gateway must be specified on Control Network A. This entry will be the same as **5a**

14k Enter the SNMP GET (read) community string.

14l Enter the SNMP SET (write) community string.

IPSI IP Addresses

15a

IP Connect
With IP Connect configurations, IP Server Interface (IPSI) circuit packs need to be manually programmed. Each Port Network (PN) will be equipped with an IPSI circuit pack. The IP addresses programmed into the IPSI circuit packs will be on the customers corporate LAN. For the purposes of these planning forms, gather enough addresses to provide one address for each ISPI.

Multi-Connect
With Multi-Connect configurations it is highly recommended that Dynamic Host Control Protocol (DHCP) be enabled on the S8700 Media Servers to assign IPSI addresses. See item **8j**.